SOPHIA FOSTER-DIMINO

Connectivity

Hijacking Computers to Mine Cryptocurrency Is All the Rage

Hackers are using old tricks and new cryptocurrencies to turn stolen computing power into digital coins.

by Mike Orcutt   October 5, 2017

Have you visited Showtime's website recently? If so, you may be
a cryptocurrency miner. An observant Twitter user was the

first to sound an alarm last month that the source code for the Showtime Anytime website contained a tool that was secretly hijacking visitors' computers to mine Monero, a Bitcoin–like digital currency focused on anonymity.

It's still not clear how the tool got there, and Showtime quickly removed it after it was pointed out. But if it was the work of hackers, the episode is actually part of a larger trend: security experts have seen a spike in cyberattacks this year that are aimed at stealing computer power for mining operations. Mining is a computationally intensive process that computers comprising a cryptocurrency network complete to verify the transaction record, called the blockchain, and receive digital coins in return (see "What Bitcoin Is, and Why It Matters").
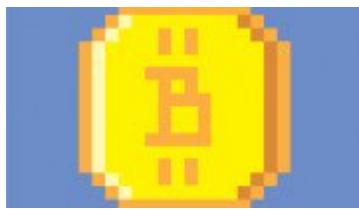
Related Story

What Bitcoin Is, and Why It Matters
Can a booming "crypto-currency" really compete with conventional cash?

Lately the same mining tool that appeared on Showtime's website has been showing up all over the Internet. Released just last month by a company called Coinhive, the tool is supposed to give website owners a way to make money without displaying ads. But malware authors seem to be among its most voracious early adopters. In the past few weeks, researchers have discovered the software hiding in Chrome extensions, hacked Wordpress sites, and even in the arsenal of a notorious "malvertising" hacker group.

Coinhive's miner isn't the only one out there, and hackers are using a variety of approaches to hijack computers. Kaspersky Lab recently reported finding cryptocurrency mining tools on 1.65 million of its clients' computers so far this year—well above last year's pace.

The researchers also recently detected several large botnets set up to profit from cryptocurrency mining, making a "conservative" estimate that such operations could generate up to $30,000 a month. Beyond that, they've seen "growing numbers" of attempts to install mining tools on servers owned by organizations. According to IBM's X-Force security team, cryptocurrency mining attacks aimed at enterprise networks jumped sixfold between January and August.

The researchers say that hackers are especially attracted to relatively new alternatives to Bitcoin, particularly Monero and zCash. That's probably in part because these currencies have cryptographic features that make transactions untraceable by law enforcement (see "Criminals Thought Bitcoin Was the Perfect Hiding Place, but They Thought Wrong"). It's also because hackers can generate more profits mining these newer currencies than they can with Bitcoin. Bitcoin-mining malware was extremely popular two or three years ago, but the currency's popularity has, by design, made it more difficult to mine, warding off this kind of attack. Hackers are now embracing newer, easier-to-mine currencies.

Sign up for **Weekend Reads**

Stories from our archives that put technology in perspective

| Your email | | **Sign Up** |

Manage your newsletter preferences

Malware containing cryptocurrency mining tools can be relatively straightforward to detect using antivirus software. cyber intelligence lead for the security firm Darkt operations set up by insiders, which can be much detect, are also on the rise, he says—often carried

The Possibility Report

An exploration of how new technologies will reframe our understanding of the world.

high-level network privileges and the technical sk[...]
their company's computing infrastructure into a [...]

Produced in partnership with VMware

In one instance, Fier's team, which relies on machine learning to detect anomalous activity inside networks, noticed an employee at a major telecom company using a company computer in an unauthorized way to communicate with his home machine. Further investigation revealed that he had planned to turn his company's server room into a mining pool.

So long as there is a potential payday involved, such inside jobs are likely to remain high on the list of cybersecurity challenges that companies face. As for keeping hacked websites from hijacking your personal computer? In an ironic twist, some ad blockers are now banning Coinhive.

Hear more about Bitcoin from the experts at the Business of Blockchain on April 23, 2018 in Cambridge.

Learn more and register

Related Video

More videos

Connectivity

Technology Spotlight: Mind-controlled VR 24:21

Connectivity

Yasmin Green: Using Technology to Make the World a Better Place 04:04

Connectivity

What is social media doing to society? 25:45

More from Connectivity

What it means to be constantly connected with each other and vast sources of information.

---

01   Ethereum's smart contracts are full of holes

Blockchain-powered computer programs promise to revolutionize the digital economy, but new research suggests they're far from secure.

by Mike Orcutt

---

02   US conservatives spread tweets by Russian trolls over 30 times more often than liberals

The first detailed analysis of how misinformation spread through the Twittersphere during the 2016 election also shows that the most retweets of troll content came from Tennessee and Texas.

by Emerging Technology from the arXiv

---

03   The Travel Ecosystem: An Industry on the Go

Amadeus, a behind-the-scenes technology provider serving the entire travel ecosystem, has transformed its technology backbone to enable the new personalized and seamless digital experiences consumers crave.

by MIT Technology Review Insights

More from Connectivity

Want more award-winning journalism? Subscribe to Insider Online Only.

Insider Online Only $9.99/3 months

Unlimited online access including articles and video, plus The Download with the top tech stories delivered daily to your inbox.

Subscribe

See details+

---

*Prices are for U.S. residents only
See international prices